LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

PIENYRITYKSEN VERKKOPALVELIN

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2013
Jori Suurnäkki

Lahden ammattikorkeakoulu
Tietotekniikka

SUURNÄKKI, JORI: Pienyrityksen verkkopalvelin

Tietoliikennetekniikan opinnäytetyö, 35 sivua, 19 liitesivua

Syksy 2013

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli tutkia Linux-käyttöjärjestelmää palvelimena ja sen tarjoamia ilmaisia avoimen lähdekoodin sovelluksia palvelinkäytössä. Työssä asennettiin verkkopalvelin, joka otetaan mahdollisesti käyttöön Päijät-Hämeen kesäyliopistolla. Verkkopalvelin tarjoaa säännölliset varmuuskopio-paketit, etähallintamahdollisuden sekä Windows workgroupissa toimivan tiedostonjakopalvelun.

Palvelimelle valittiin käyttöjärjestelmä kolmesta Linux-jakelusta. Käyttöjärjestelmää valittaessa keskityttiin kustannustehokkuuteen ja tietoturvaan. Palvelimelle asennetaan Samba-palvelu, jonka avulla liitettiin Linux-palvelin Windowsin workgroupiin ja käyttäjien tiedostoista ja käyttöjärjestelmistä otettiin varmuuskopiot. Palvelinta hallitaan etänä terminaalipohjaisen etähallinnan avulla.

Käytännön toteutuksessa asennettiin palvelimelle CentOS-käyttöjärjestelmä. Palvelimelle asennettiin myös Samba-palvelu, jonka avulla luotiin käyttäjille yhteiset ja henkilökohtaiset kansiot verkkopalvelimelle. Palvelimeen konfiguroitiin SSH-etähallintamahdollisuus sekä toteutettiin varmuuskopiointipalvelu cron-ajastusohjelman avulla.

Tämän työn tuloksena saatiin Linux-pohjainen palvelin Windows workgroup -ympäristöön. Palvelimella käytetään Samba-palvelua tiedostojen jakoon, joita varmuuskopioidaan cron-ajastusohjelmaan luodun pakkauskomennon avulla. Palvelinta voidaan hallita etänä SSH-protokollan avulla.

Asiasanat: Samba, Linux, varmuuskopio, Windows, workgroup

Lahti University of Applied Sciences
Degree Programme in Telecommunications Technology

SUURNÄKKI, JORI: Server for a small business

Bachelor's Thesis in telecommunications, 35 pages, 19 pages of appendices

Autumn 2013

ABSTRACT

The goal of the thesis was to examine the Linux-based operation system as a server and the free open source software in server usage. The thesis presents the installation of a workgroup server which might be used in the Summer University of Päijät-Häme. The function of the server is to provide backups on a daily basis, operational remote control and a shared file server in the workgroup.

Three Linux distributions were reviewed, one of which was chosen for the server's operating system. When choosing the operating system the focus was on cost-efficiency and information security. The Linux server was connected to the Windows workgroup via the Samba service. Backups were taken of users' files and the Windows operating systems. The server is remotely controlled with terminal-based software.

The CentOS operating system was installed on the server. Samba service was also installed, which is used to create common and private folders on the server. SSH remote connection was configurated to the server and backup services are provided with cron, time-based job scheduling software.

The result of this work is a Linux-based server on a Windows workgroup. The server is using Samba service for sharing files which are backed up using a script in cron scheduling software. The server can be controlled remotely using the SSH protocol.

Key words: Samba, Linux, backup, Windows, workgroup

SISÄLLYS

LYHENNELUETTELO

AD	Active Directory. Windowsin hakemistopalvelujärjestelmä.
APT	Advanced Package Tool. Työkalu paketinhallinnan helpottamiseksi Debian-jakelussa.
CIFS	Common Internet File System. Protokolla, jota käytetään tiedostojen jakamiseen verkossa.
GNU	GNU’s Not Unix. Richard Stallmanin luoma projekti täysin vapaan Unix-pohjaisen käyttöjärjestelmän kehittämiseen.
GNU GPL	GNU General Public License. Yleisin lisenssi, jota käytetään avoimen lähdekoodin ohjelmistoissa.
IETF	Internet Engineering Task Force. Organisaatio, joka vastaa Internet-protokollien standardoinnista.
IP	Internet Protocol. TCP/IP-mallin Internet-kerroksen protokolla.
IPSec	Internet Protocol Security. IPSec on protokollajoukko, jota käytetään IP-paketin turvaamiseen.
LAN	Local Area Network. Lähiverkko.
NTLM	NT LAN Manager. Sisältää Microsoftin turvallisuusprotokollia.
OSI-Malli	Open Systems Interconnection Reference Model. ISO:n luoma kansainvälinen malli, joka kuvaa datan siirtymistä tietoverkossa seitsemän tiedonsiirtoprotokollia käsittelevän kerroksen avulla.

RAID	Redundant Array of Independent Disks. Tietokoneen kiintolevyjen kanssa käytettävä tekniikka, jolla voidaan parantaa lukunopeutta ja vikasietoisuutta.
rlogin	Ohjelmisto Unixin kaltaisille käyttöjärjestelmille, jolla voidaan luoda etäyhteys verkon yli järjestelmien välille.
RPM	RPM Package Manager. Paketinhallintajärjestelmä, jota käytetään useissa Linux-jakeluissa.
rsh	Remote shell. Ohjelmisto, jonka avulla voidaan suorittaa shell-komentoja toisena käyttäjänä sekä luoda etäyhteys verkon yli järjestelmien välille.
SFTP	SSH File Transfer Protocol. Turvallinen tiedonsiirtomenetelmä kahden tietokoneen välille.
Shell	UNIX-pohjaisen käyttöjärjestelmän komentorivi.
SMB	Server Message Block. Protokolla, jota käytetään tiedostojen jakamiseen verkossa.
SSH	Secure Shell. Protokolla, jonka avulla voidaan luoda salattuja yhteyksiä järjestelmien välille.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jota käytetään luomaan yhteyksiä tietokoneiden välille.
VPN	Virtual Private Network. Julkisen verkon yli luotu useamman verkon tai etäkäyttäjän välinen näennäinen yksityisverkko.
WINS	Windows Internet Name Service. WINS muuttaa tietokoneen NetBIOS-nimet IP-osoitteiksi.

YUM	Yellow Dog Updater, Modified. Muun muassa RHEL-pohjaisissa Linux-jakeluissa käytettävä komentorivipohjainen paketinhallintatyökalu.

1 JOHDANTO

Päijät-Hämeen kesäyliopistolta puuttuu tällä hetkellä Windowsin workgroupissa toimiva verkkopalvelin, jossa olisi hyvät etähallintamahdollisuudet sekä tiedostonjakopalvelu käyttäjille.

Päijät-Hämeen kesäyliopisto on yksi Suomen kahdestakymmenestä kesäyliopistosta, ja se on toiminut jo vuodesta 1962. Kesäyliopiston toimipiste sijaitsee Lahden aikuiskoulutuskeskuksessa, ja Päijät-Hämeen kesäyliopistot ry vastaa oppilaitoksen ylläpidosta. Päijät-Hämeen kesäyliopiston toiminta pohjautuu kesäyliopiston johtokunnan hyväksymään strategiaan. (Päijät-Hämeen kesäyliopisto 2013.)

Opiskelijoille tarjotaan ajankohtaisia ja laadukkaita kursseja ympäri vuoden. Päijät-Hämeen yliopisto järjestää opiskelijoilleen avoimen yliopisto-opetuksen lisäksi kielikoulutusta, lukiolaiskursseja sekä ammatillista täydennyskoulutusta. Opiskelijoita Päijät-Hämeen kesäyliopistossa on vuosittain 2300 - 3400. (Päijät-Hämeen kesäyliopisto 2013.)

Tämän opinnäytetyön tavoitteena on luoda pienyritykselle Linux-pohjainen malli mahdollisesta verkkopalvelimesta, jonka yhtenä päätehtävänä on toimia yhteisenä tiedostopalvelimena käyttäjille. Samalla tutustutaan Linux-pohjaisen palvelimen mahdollisuuksiin ja avoimen lähdekoodin sovellusratkaisuihin.

2 PALVELIMEN KÄYTTÖJÄRJESTELMÄ – LINUX

Linux sai alkunsa vuonna 1991, kun helsinkiläinen opiskelija Linus Torvalds ei ollut tyytyväinen silloisen tietokoneensa käyttöjärjestelmään ja päätti lopulta kehittää oman. Alun perin omaan käyttöön kehitetty käyttöjärjestelmä muokkaantui yhdeksi maailman suosituimmaksi palvelinkäyttöjärjestelmäksi. (Wikipedia 2013c; Wikipedia 2013e.)

Pelkkä Linux ei kuitenkaan tarkoita käyttöjärjestelmää, vaan kerneliä eli ydintä. Ydin toimii rajapintana ohjelmistojen ja tietokoneen osien välillä. Linux-kernelin ympärille on koottu käyttöjärjestelmä GNU GPL -lisenssin alaisista vapaan ja avoimen lähdekoodin ohjelmistoista. Siksi käyttöjärjestelmään viitatessa käytetään termiä GNU/Linux. (Stallman 2007; Linux 2013c.)

Linuxin pohjautuminen vapaaseen ja avoimeen lähdekoodiin on toiminut ponnahduslautana usealle uudelle Linux-jakelulle. Eniten ohjelmistopaketteja on tarjolla Ubuntulle ja Debianille. (Wikipedia 2013a.)

2.1 CentOS

CentOS on kustannustehokas Linux-jakelu, joka tarjoaa ilmaisen yritystason käyttöjärjestelmän. CentOS pohjautuu kaupalliseen Red Hat Enterprise Linuxiin (RHEL) ja ovat täten binääriyhteensopivia. Ensimmäinen CentOS-julkaisu, CentOS-2, ilmestyi vuonna 2004, joka pohjautui RHEL:n vuonna 2002 ilmestyneeseen 2.1AS-julkaisuun. (CentOS-2 2006; Linux 2013a.)

CentOS käyttää YUM-paketinhallintatyökalua RPM-pakettien hallintaan. CentOS-käyttöjärjestelmästä on mahdollista ladata niin graafinen kuin minimalistisempikin versio. Minimal-versio sisältää tarvittavan määrän paketteja, joilla voidaan luoda toimiva käyttöliittymä. Minimal-versio ei kuitenkaan sisällä graafista käyttöliittymää, ja sitä hallitaan komentorivin kautta. (CentOS 2013; Linux 2013a; The CentOS Project 2013.)

2.2 Debian

Ian Murdock perusti The Debian Projectin vuonna 1993, jonka myötä julkaistiin ensimmäinen Debian GNU/Linuxin jakelu. Debian on yksi vanhimmista Linux-jakeluista ja tämän vuoksi myös yksi tuetuimmista. Debianissa on laaja prosessorituki sekä ohjelmistopakettivalikoima. Debian tarjoaakin täysin ilmaisen avoimeen lähdekoodiin perustuvan käyttöjärjestelmän, jonka kaikki ohjelmistot ovat saatavina ilmaiseksi. Tämän vuoksi Debian onkin ollut pohjana usealle eri Linux-jakelulle. (Debian Documentation Team 2013; Debian GNU/Linux FAQ 2013; Wikipedia 2013b.)

Debianin paketinhallintajärjestelmä on nimeltään dpkg, jonka samanniminen komentorivipohjainen työkalu mahdollistaa deb-muotoisten pakettien poistamisen, asentamisen ja päivittämisen. Paketinhallinnan helpottamiseen Debian Project on kehittänyt apt-työkalun, jonka avulla huolehditaan asennuspakettien hakemisesta ja riippuvuussuhteista. (Linux 2013b; Debian Wiki 2013.)

2.3 Ubuntu

Ubuntu on Debianiin pohjautuva Linux-jakelu, joka mainostaa itseään käyttäjäystävällisenä ja työpöytäkäyttöön soveltuvana käyttöjärjestelmänä. Ubuntun ensimmäinen julkaisu oli vuonna 2004. Ubuntun takana on monimiljönääri Mark Shuttleworth, jonka perustama yritys Canonical Ltd. vastaa tällä hetkellä Ubuntun kehitystoiminnasta. Ubuntusta on olemassa erikseen omat julkaisut työpöytäkäyttöön (Ubuntu Desktop) sekä palvelinkäyttöön (Ubuntu Server). Ubuntu on laajentanut markkinoitaan ja esitellyt tulevia käyttöliittymiä myös älypuhelimiin (Ubuntu Touch, Ubuntu for Android), tabletteihin (Ubuntu Touch) sekä smart-televisioihin (Ubuntu TV). (Ubuntu 2013; Wikipedia 2013l.)

Ubuntu käyttää samaa paketinhallintajärjestelmää dpkg kuin Debian. Paketinhallintatyökaluna Ubuntulla on apt. Ubuntusta on saatavilla myös kouluympäristöön suunniteltu jakelu Edubuntu. Edubuntu voidaan myös asentaa lisäosana Ubuntu-jakeluun. (Wikipedia 2013l.)

3 VERKKOPALVELIMEN PALVELUT

3.1 Samba

Samba on vuonna 1991 alkunsa saanut avoimen lähdekoodin ohjelma, jonka avulla voidaan mahdollistaa Unix-johdannaisten ja Windows-pohjaisten käyttöjärjestelmien välinen tiedonsiirto ja tulostimien jako. Samba käyttää CIFS-protokollaa, joka toimii TCP/IP-protokollan päällä. Samballa on mahdollista toteuttaa useita erilaisia palveluja, joista yleisimpiä ovat seuraavat:

- hakemistojen jakaminen
- tulostimien keskitetty jako Windows-asiakkaille
- käyttäjien verkkoympäristön selailun helpottaminen
- WINS-nimipalvelun hyödyntäminen
- Windows-domainiin kirjautuvien asiakkaiden autentikointi
- DFS-nimiavaruuden tarjoaminen.

Samban kolme keskeisintä UNIX-taustapalvelua ovat smbd, nmbd ja winbindd. Näistä smbd hallitsee tiedosto- ja tulostinjaot ja SMB-asiakaskoneiden tunnistautumisen. Nmbd puolestaan vastaa Samban NetBIOS-nimipalvelusta, joka on Microsoftin kanssa yhteensopiva. Nmbd on käytännössä sama Samballe, kuin mitä WINS on Windowsille. Winbindd puolestaan yhtenäistää Windowsin domain controllerilta saadut käyttäjä- ja ryhmätiedot UNIX-järjestelmän kanssa. Winbindd tarjoaa myös rajapinnan NTLM-autentikointiin muiden UNIX-palveluiden kanssa. (Collier-Brown, Eckstein & Ts 2007, 2 - 3.)

3.1.1 Samba stand-alone-palvelimena

Sambaa voidaan käyttää stand-alone-palvelimena. Tällöin Windows-verkossa oleva Samba-palvelin ei kuulu Windowsin toimialueeseen eikä sitä voida hallita Windowsin toimialueen sisällä. Kun Samba toimii stand-alone-palvelimena, se näkyy Windowsin verkossa yhtenä Windowsin työryhmän (workgroup) tietokoneena. Samba stand-alone -palvelinta voidaan siis sanoa myös workgroup-palvelimeksi. Workgroupissa tiedostojen jakaminen on yksinkertaista ja helppoa, kunhan verkko on kooltaan pieni ja käyttäjiä on vähän. Samban toimiessa

workgroup-palvelimena täytyy palvelimen ylläpitäjän lisätä käyttäjälle käyttäjätunnus ja salasana Samban tietokantaan. (Collier-Brown ym. 2007, 23, 234.)

3.1.2 Samba Windowsin domainissa

Samba-palvelin voi toimia Windowsin toimialueella jäsenenä sekä domain controllerina. Samba on myös yhteensopiva Windowsin AD-järjestelmän kanssa. Sambasta löytyvän winbind-palvelun avulla Windows-käyttäjät pääsevät käsiksi Samba-palvelimella oleviin jaettuihin tiedostoihin käyttämällä omaa Windows toimialueen salasanaa ja käyttäjätunnusta. Winbind-palvelu mahdollistaa siis Samba-palvelimeen pääsyn ilman lokaaleja käyttäjätunnuksia. (Collier-Brown ym. 2007, 23 - 25, 286.)

3.2 Palvelimen tiedostojen varmuuskopiointi

Tiedostojen varmuuskopioiminen on tärkeä osa palvelimen ylläpitoa. Varmuuskopioinnilla eli backupilla varmistetaan, että käyttäjien tiedostot eivät häviä koneelta mahdollisten ongelmien takia. Yleisiä ongelmia, joita käyttäjille voi sattua tiedostojen kanssa:

- Käyttäjä poistaa huolimattomuuttaan tiedoston tai tekee jonkun muun vastaavan inhimillisen virheen.
- Tiedostot voivat korruptoitua.
- Kiintolevyt voivat hajota tai ne mahdollisesti varastetaan.

Käyttäjän on hyvä omistaa useita eri medioita, joihin voi tallentaa omat varmuuskopionsa. Varmuuskopioita olisi aina hyvä olla useampi ja useassa eri paikassa mahdollisten tapaturmien vuoksi. (Cibernarium 2005.)

3.2.1 RAID

RAID on tiedonvarastointitekniikka, jolla parannetaan suorituskäyttöä ja vikasietoisuutta yhdistämällä useita fyysisiä levyjä loogisiksi kokonaisuuksiksi.

Yleisimmät RAID-tekniikat:

- RAID0-tekniikassa kovalevyt yhdistetään yhdeksi loogiseksi kovalevyksi. Data jakautuu tasaisesti kaikille levyille, joten yhden levyn hajotessa koko pakan data menetetään.
- RAID1-tekniikassa peilataan levyt, eli tallennetaan usealle erilliselle levylle.
- RAID0+1 yhdistelee RAID0- ja RAID1-tekniikkaa ja tarvitsee vähintään 4 levyä toimiakseen. RAID0+1-tekniikassa loogiset kokonaisuudet peilataan.
- RAID1+0 eli RAID10 on RAID01-tekniikan vastakohta. Siinä peilatut levyt muodostavat loogisen kokonaisuuden
- RAID5 käyttää pariteettilaskentaa ja hajauttaa pariteettibitit kaikille levyille. Koko pakka ei vielä hajoa, jos yksi levy hajoaa. (The Raid Tutorial 2013.)

3.2.2 Tar & Duplicity

Tar on komentoriviltä suoritettava työkalu yksinkertaisten tar-pakettien luomiseen. Tar on lyhenne sanoista Tape Archive. Tar-pakettimuoto ei itsessään pakkaa dataa pienempään kokoon, vaan sillä kootaan valitut tiedostot yhdeksi tar-paketiksi. Kun tar-ohjelmistoa käytetään varmuuskopioimiseen, se yleensä pakataan gzip- tai bzip2-ohjelmistoilla. (Linux 2013c; Wikipedia 2013k.)

Duplicity on rsync-algoritmiin perustuva ilmainen GNU GPL-lisenssillä varustettu varmuuskopiointiohjelma, jolla voi luoda salattuja, digitaalisesti allekirjoitettuja ja etäbackupeja. Duplicity toimii rsync-ohjelmiston tavoin luoden ensin täydellisen backupin, jonka jälkeen seuraavissa backupeissa tallennetaan vain ne tiedostot, jotka ovat muuttuneet. (Duplicity 2013.)

3.3 Etäyhteys

3.3.1 SSH

Secure Shell -protokolla eli SSH on Tatu Ylösen vuonna 1995 kehittelemä merkkipohjainen etähallintaprotokolla, jonka avulla luodaan turvallinen etäyhteys verkon yli serverin ja asiakasohjelman välille. Ensimmäinen versio SSH:sta (SSH-1) suunniteltiin telnet-, rlogin- ja rsh-yhteysprotokollien korvikkeeksi lähinnä niiden heikon tietoturvan ja salaamattoman yhteyden takia. Telnetin, rloginin ja rsh:n käyttö onkin vähentynyt radikaalisti ja SSH-protokolla on käytännössä korvannut nämä. (RFC 4252 2006; Wikipedia 2013i.)

SSH:n ensimmäisestä versiosta löytyvien ongelmien ja rajoittuvuuksien takia SSH-protokollasta kehitettiin uudempi versio vuonna 1996, SSH-2, joka sisältää niin tietoturvallisia kuin toiminnallisiakin parannuksia ensimmäiseen versioon verrattuna. Vuonna 2006 SSH-2-protokolla määriteltiin IETF:ssä aiotuksi uudeksi Internet standardiksi. SSH-2-protokollan turvallisuuden ja toiminnallisen paremmuuden takia SSH-1-protokollan käyttöä on vähennetty. (Barrett, Silverman & Byrnes 2005, 9; RFC 4250 2006.)

SSH toimii OSI-mallin seitsemännellä kerroksella eli sovelluskerroksella ja käyttää TCP:n porttia 22. Yhteyden salaamiseen SSH käyttää julkisen avaimen salausta tunnistautuakseen etälaitteen kanssa. Yksi yleinen tapa kirjautua SSH:n kautta koneelle on tunnistautua SSH:n luoman avainparin kanssa, jolla salataan käytettävä verkkoyhteys, jonka jälkeen voidaan kirjautua käyttäjänimellä ja salasanalla sisälle. Toinen yleinen tapa on luoda oma avainpari käytettävien laitteiden kanssa, jolloin ei välttämättä tarvita salasanaa kirjautumiseen. (IANA 2013; RFC 4252 2006; Wikipedia 2013h.)

SSH-protokollaa voidaan käyttää useiden eri ohjelmistojen ja käyttöjärjestelmien kanssa. Muutamia hyviä esimerkkejä SSH-protokollan hyödyntämisestä:

- isäntäkoneen shelliin kirjautuminen, jonka avulla voidaan hallita konetta etänä
- turvallinen tiedostojen siirto verkon yli, esimerkiksi SFTP:tä hyödyntäen

- portin tunnelointi SSH:n avulla, jolloin käyttäjä voi välittää suojaamatonta liikennettä SSH:n tunnelin avulla. (Wikipedia 2013h.)

3.3.2 VPN

VPN eli Virtual Private Network tarkoittaa useamman verkon tai käyttäjän yhdistämistä julkisen verkon esim. Internetin yli omaksi näennäiseksi yksityiseksi verkoksi. VPN:stä käytetään kahdenlaista topologiaa: etäyhteyttä (remote-access) tai kahden verkon välistä yhteyttä (LAN-to-LAN). Yrityksissä halutaan taata käyttäjille pääsy yrityksen sisäiseen verkkoon ja sitä kautta yrityksen yhteisiin tiedostoihin, niin etänä käyttäjälle, kuin toiselle geografisesti eri paikassa sijaitsevalle yritykselleKin. VPN:n avulla tällainen julkisen verkon yli työskentely on tietoturvallista sekä kustannustehokasta yrityksen kannalta. (Microsoft TechNet 2001; VPNC 2008.)

Kahden päätelaitteen, verkko-verkko tai tietokone-toimisto, välinen VPN-liikenne tunneloidaan verkossa liikkuvan datan turvaamiseksi. Esimerkiksi IPSec-protokollakokoelmaa hyödyntäessä IP-paketti etenee VPN-tunnelissa IPSec-paketin sisällä. VPN-tunneleista saadaan turvallisia erilaisilla tunnistautumismenetelmillä. Kahden verkon välisessä VPN-tunnelissa käytetään yleensä ennaltamäärättyjä avaimia (vähän niin kuin SSH:ssa) tai digitaalisia sertifikaatteja. Nämä digitaaliset sertifikaatit toimivat kuin avaimet, mutta sisältävät digitaalisen allekirjoituksen. (Microsoft TechNet 2001; Wikipedia 2013m; Wikipedia 2013b.)

Etäkäyttäjän yhdistäessä yrityksen VPN-serveriin etäkäyttäjällä on yleensä käytössä jonkinlainen VPN-sovellus. Yhdistettäessä käyttäjä voi tunnistautua omalla käyttäjätunnuksella ja salasanalla ja tieto lähetetään eteenpäin serverille. Jos VPN-serverillä on olemassa privaatti osoiteavaruus VPN-käyttäjille, antaa VPN-serveri käyttäjälle privaatista osoiteavaruudesta osoitteen, jonka avulla käyttäjä pääsee käsiksi oman yrityksen verkkoon. (Microsoft TechNet 2001; Wikipedia 2013m.)

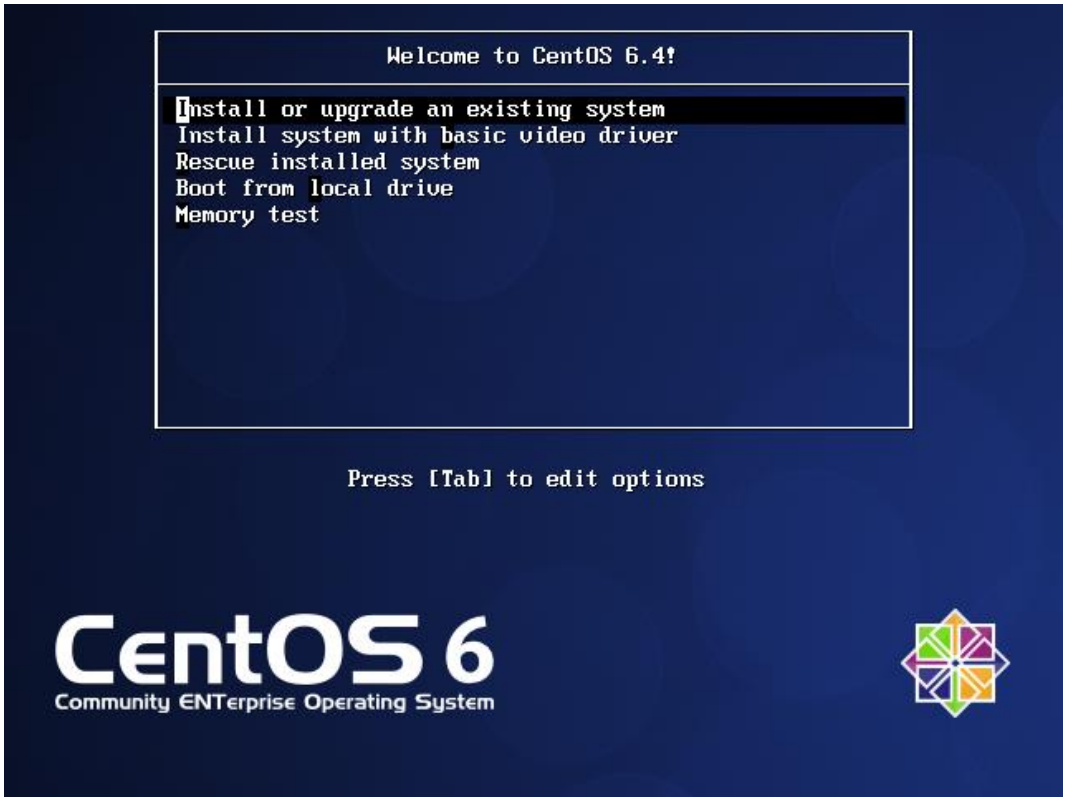
4 VERKKOPALVELIMEN SUUNNITTELU JA TOTEUTUS

Tässä työssä luodaan verkkopalvelimen malli, joka voidaan ottaa käyttöön tulevaisuudessa Päijät-Hämeen kesäyliopistolla. Verkkopalvelinta suunniteltaessa haluttiin valita palveluista järkevin toteutus, joka ei kuitenkaan ylikuormittaisi palvelinta. Palvelimeen haluttiin myös palveluiden laajennusmahdollisuus tulevaisuutta ajatellen ja turvallinen etähallintajärjestelmä.

4.1 Käyttöjärjestelmän asennus

Käyttöjärjestelmää valittaessa kiinnitettiin huomiota käyttöjärjestelmän vakauteen sekä käyttöjärjestelmän palvelinominaisuuksiin. Käyttöjärjestelmä valittiin kolmesta Linux-jakelusta, jotka olivat Debian, Ubuntu ja CentOS. Vaikka Debiania ja Ubuntua pidetään enemmän työpöytäkäyttöön tarkoitettuina käyttöjärjestelminä, sisältävät molemmat jakelut hyviä palvelinkäyttöön tarkoitettuja ohjelmistoja. Ubuntusta on myös julkaistu Ubuntu Server, joka on palvelinkäyttöön tarkoitettu käyttöjärjestelmä. Debian-, Ubuntu- ja CentOS-jakelut ovat myös todella vakaita, koska jakeluversioiden hitaan julkaisusyklin vuoksi palvelinta ei tarvitse päivittää niin tiheästi. Näistä kolmesta CentOS on kuitenkin eniten yrityskäyttöön suunniteltu käyttöjärjestelmä. Tämä oli yksi niistä syistä, miksi käyttöjärjestelmäksi lopulta valikoitui CentOS-jakelu. Valintaan vaikutti myös CentOS-käyttöjärjestelmän hyvät palvelinominaisuudet sekä aiempi kokemus CentOS-käyttöjärjestelmästä.

Koska verkkopalvelimella ei tarvita graafista käyttöliittymää, valittiin asennettavaksi versioksi 6.4 Minimal. Käyttöjärjestelmä asennettiin CD-levyltä. Asennus aloitettiin valitsemalla **Install or upgrade an existing system** kuvion 1 mukaan. (Kuvio 1.)

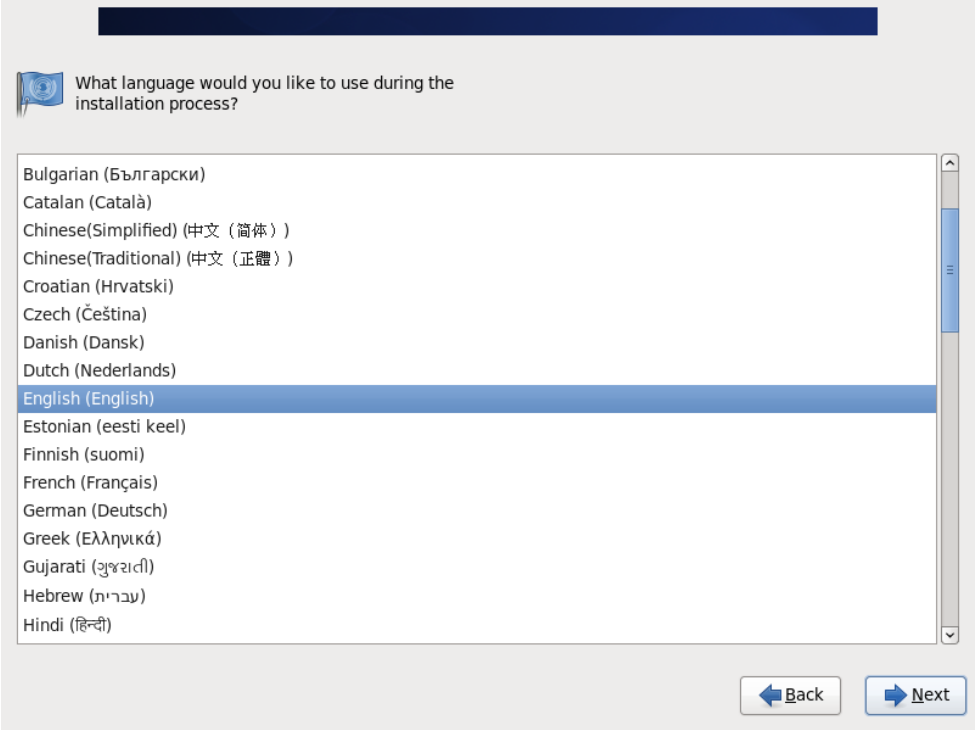


KUVIO 1. CentOS-asennus: Asentamisen aloittaminen

Disc found -kohdassa valitaan Skip. Mediaa ei tarvitse testata. (Kuvio 2.)

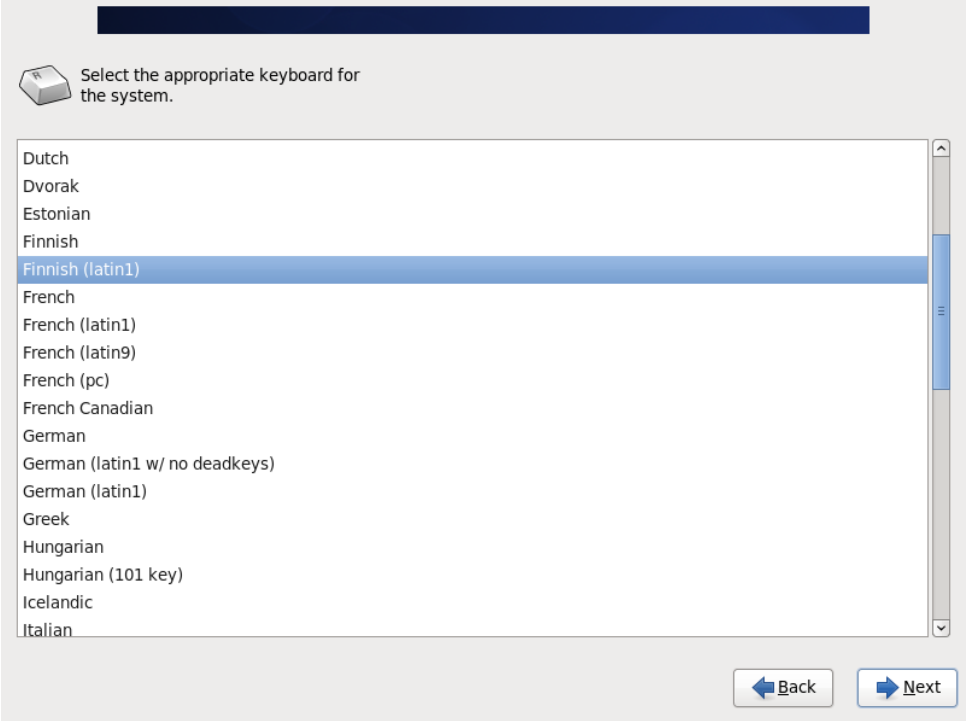
KUVIO 2. Centos-asennus: Media test

Asennuskieleksi valitaan englanti (kuvio 3).



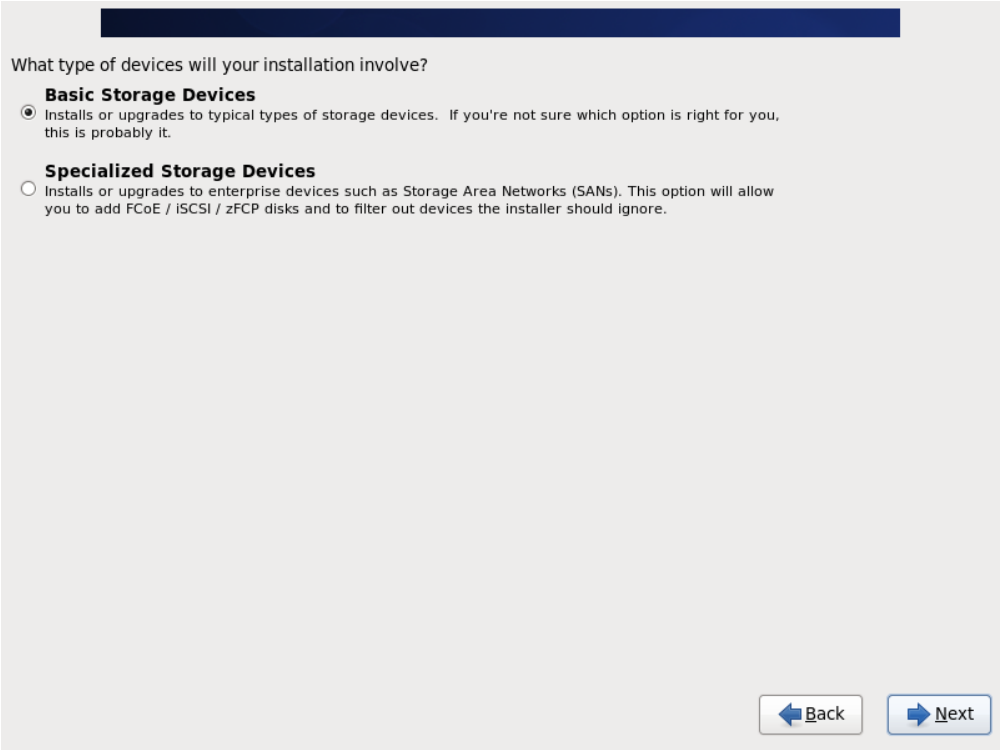
KUVIO 3. Centos-asennus: Asennuskielen valitseminen

Näppäimistötyypiksi valitaan Finnish (latin1) (kuvio 4).



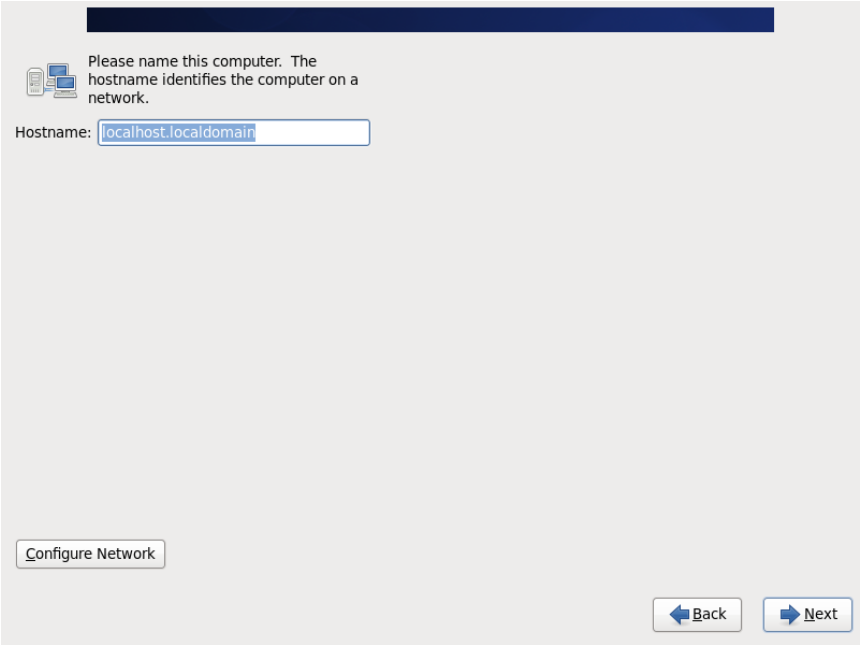
KUVIO 4. Centos-asennus: Näppäimistöasetukset

Seuraavaksi valitaan Basic Storage Devices, sillä palvelimen käytössä ei ollut alla mainittuja tallennusratkaisuja (kuvio 5).



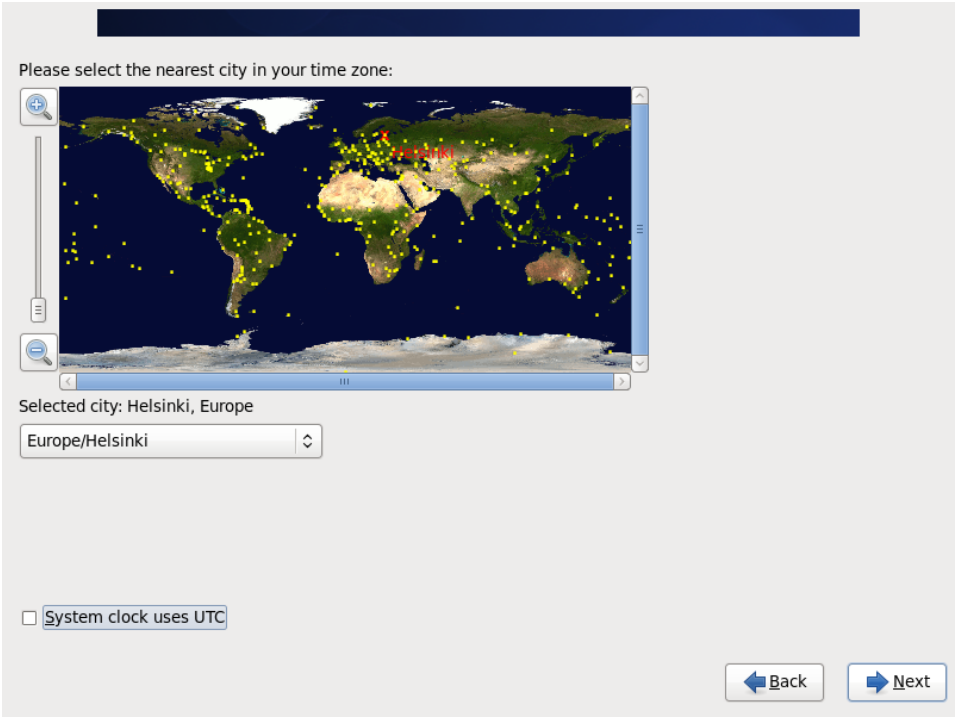
KUVIO 5. Centos-asennus: Tallennusvälinetyypin valitseminen

Seuraavaksi määriteltiin palvelimen hostname. Koska hostnamen voi vaihtaa myöhemminkin konfiguraatioista, niin sitä ei ole vielä pakollista vaihtaa. (Kuvio 6.)



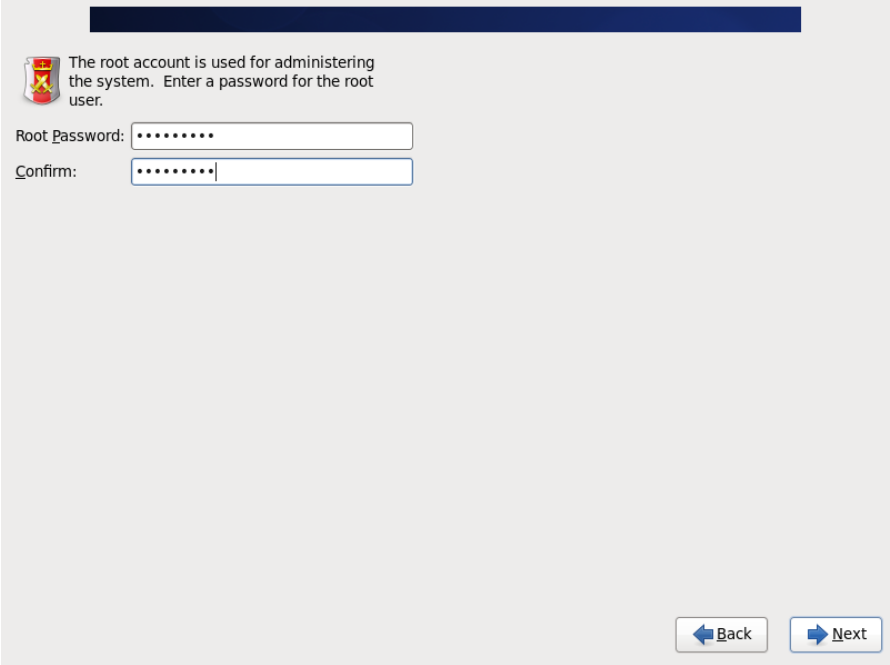
KUVIO 6. Centos-asennus: Hostnamen valitseminen

Seuraavaksi valittiin oikea aikavyöhyke eli Europe/Helsinki. Samalla otettiin ruksi pois kohdasta System clock uses UTC. (Kuvio 7.)



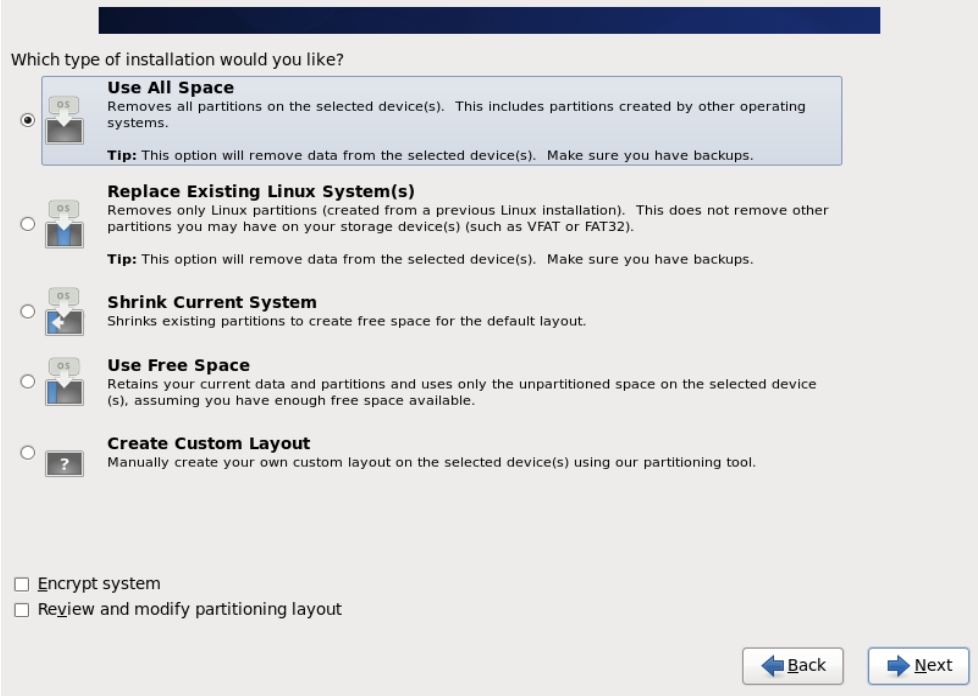
KUVIO 7. Centos-asennus: aikavyöhykkeen valitseminen

Seuraavaksi määriteltiin salasana root-tunnukselle (kuvio 8).



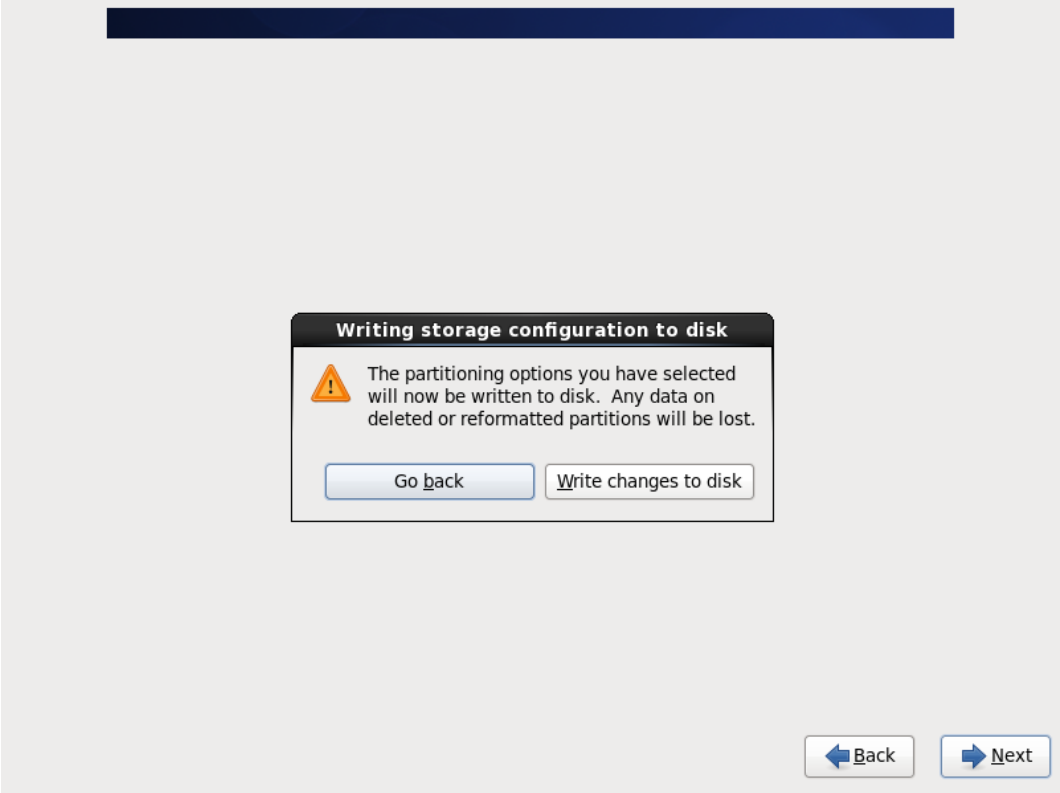
KUVIO 8. Centos-asennus: Root-tunnuksen salasanan laittaminen

Seuraavaksi valittiin, kuinka käyttöjärjestelmä asennetaan palvelimelle. Koska haluttiin aloittaa asennus tyhjälle kovalevylle, valittiin Use All Space. (Kuvio 9.)



KUVIO 9. Centos-asennus: Asennustapa

Seuraavaksi tuli varmistusilmoitus, että halutaanko varmasti ajaa tallennuslaite tyhjäksi ennen käyttöjärjestelmän asennusta. Valitaan write changes to disk. (Kuvio 10.)



KUVIO 10. CentOS-asennus: Varmistusilmoitus levyjen tyhjentämisestä

Tämän jälkeen CentOS asentui palvelimelle. Seuraavaksi kirjaudutaan sisään root-tunnuksilla. Ensimmäisenä luodaan uusi käyttäjäryhmä nimeltä hallinta komennolla:

groupadd hallinta

Sitten luodaan käyttäjätunnus admin1 ja liitetään se ryhmään hallinta, jonka jälkeen luodaan käyttäjätunnukselle salasana

useradd –g hallinta admin1

passwd admin1

Seuraavaksi muokataan Vi-tekstieditorilla eth0-verkkokortin asetukset kuntoon. Avataan määritystiedosto komennolla:

vi /etc/sysconfig/network-scripts/ifcfg-eth0

Koska työssä käytettiin koulun tietoverkkolaboratorioon luotua testiympäristöä, syötettiin ip-osoite verkosta 193.166.74.0.

DEVICE=eth0

IPADDR=193.166.74.99

NETMASK=255.255.255.128

NETWORK=193.166.74.0

BROADCAST=193.166.74.127

TYPE=Ethernet

ONBOOT=yes

NM_CONTROLLED=no

BOOTPROTO=none

USERCTL=no

Jotta testiverkko saataisiin toimimaan, määriteltiin seuraavaksi DNS-palvelimien osoitteet. Avataan vi-editorissa tiedosto:

vi /etc/resolv.conf

Ja muokataan tiedosto seuraavasti:

nameserver 193.167.119.9

nameserver 193.167.119.8

search lpt.fi

Seuraavana määriteltiin oletusreititin ja tämän jälkeen verkkoasetukset ovat kunnossa. Avataan vi-editorissa tiedosto:

vi /etc/sysconfig/network

Lisätään tiedostoon oletusreititin ja samalla voidaan lisätä haluamamme hostname:

NETWORKING=yes

GATEWAY=193.166.74.1

HOSTNAME=phkesayo

Jotta verkkoasetukset saadaan voimaan, täytyy verkkopalvelu käynnistää uusiksi komennolla:

service network restart

Tämän jälkeen voidaan testata verkon toimivuutta esimerkiksi pingaamalla googlen palvelimelle komennolla ping www.google.fi

Kun verkko toimii, ladataan päivitykset käyttöjärjestelmään komennolla:

yum –y update

Päivitysten jälkeen asennetaan vi-tekstieditorin tilalle toinen tekstieditori nano komennolla:

yum install nano

Seuraavaksi otetaan vielä SELinux pois käytöstä, sillä sitä ei tulla tarvitsemaan. Avataan SELinuxin konfiguraatiotiedosto komennolla:

nano /etc/selinux/config

Sitten muutetaan enforced-tilan paikalle:

SELINUX=disabled

Näin konfiguroidaan onnistuneesti verkkoasetukset.

Käyttäjätilien ja -ryhmien luonti

Seuraavaksi luodaan Päijät-Hämeen kesäyliopiston työntekijöille oma ryhmä ja jokaiselle työntekijälle oma tunnus. Testiympäristöön luodaan viidelle työntekijälle käyttäjätunnukset ja näille viidelle henkilölle yksi yhteinen ryhmä. Kirjaudutaan sisään root-käyttäjänä ja luodaan yhteinen ryhmä komennolla:

groupadd phkesayo

Seuraavaksi luodaan viisi käyttäjätunnusta komennolla, jossa X=1-5:

useradd –g phkesayo phkesayo_userX

Tämän jälkeen luodaan jokaiselle käyttäjälle salasanat, esimerkiksi käyttäjälle phkesayo_user1:

passwd phkesayo_user1

Salasanaksi voidaan antaa jokaiselle käyttäjälle sama kuin mitä käyttäjätunnus on, joten salasanojen muistaminen on helppoa.

Luodaan vielä testausmielessä yksi admin-tunnus nimellä tvlabra hallintaryhmään komennolla:

useradd –g hallinta tvlabra

4.2 Etäyhteyden mahdollistaminen

Verkkopalvelimelle halutaan turvallinen etähallintamahdollisuus. Tätä varten luodaan palvelimelle toimiva SSH. Palvelimelle piti asentaa myös IPSec-protokollaa hyödyntävä VPN-yhteys, mutta valitettavasti sen luomisessa ei onnistuttu. Ongelmaksi muodostuivat huonot sovellusvalinnat sekä VPN-tunnelointiin liittyvä ongelma testiympäristössä, joten mahdollisten konfiguraatioiden toimivuuden todentaminen oli hankalaa. Aluksi kokeiltiin OpenSwan-ohjelmistoa, jonka avulla voidaan luoda mm. IPSec-protokollaa hyödyntäviä etäratkaisuja. Verkkoliikenteen seuraamiseen käytettiin tcpdump-

ohjelmistopakettia, jonka avulla voidaan tutkia verkkoliikenteessä kulkevia paketteja. Useiden eri konfiguraatiokokeilujen jälkeen yhtään lähtevää IPSec-pakettia ei onnistuttu luomaan. Ajanpuutteen vuoksi ei keretty kokeilemaan toista IPSec-protokollaa hyödyntävää etäratkaisua nimeltä StrongSwan. StrongSwanin sivuilta löytyvät ainakin paremmat dokumentaatiot, joiden avulla voisi konfiguroiminen olla helpompaa.

Koska VPN-tunnelointia ja IPSec-protokollaa ei saatu toimimaan, tapahtuu etäyhteyden ottaminen SSH-protokollan avulla. SSH-protokollan konfiguroiminen aloitetaan muokkaamalla SSH:n konfiguraatioita. Kirjaudutaan root-käyttäjänä sisään ja avataan SSH:n konfiguraatiotiedosto nano-tekstieditorilla seuraavasti:

nano /etc/ssh/sshd_config

Sitten laitetaan seuraavat asetukset käytäntöön:

Protocol 2

Tällä sallitaan yhteydenotot vain SSH-versiolla 2.

PermitRootLogin no

Tämä komento estää sen, että SSH-yhteyttä ei voi avata root-tunnuksella.

StrictModes yes

SSH tarkistaa käyttäjän oikeudet omaan kotikansioon ja rhosts-tiedostoihin ennen sisäänkirjautumista.

IgnoreRhosts yes

SSH määrittää, estetäänkö rhosts- tai shosts-tiedostojen käyttö autentikoimisessa.

PermitEmptyPasswords no

Tämä määrittää, voiko SSH:n yli kirjautua käyttäjätunnuksiin tyhjällä salasanalla.

X11Forwarding no

SSH-tunnelin yli ei voida avata graafista X11-yhteyttä.

Tallennetaan tehdyt muutokset ja suljetaan nano-tekstieditori. Nyt kirjautuminen suoraan roottina SSH:n yli on estetty, joten kirjautuminen tehdään peruskäyttäjän tunnuksella.

Seuraavaksi muokataan palomuuriasetukset kuntoon. Käytetään taas nano-tekstieditoria palomuurin konfiguraatiotiedoston avaamiseen. Suoritetaan komento:

nano /etc/sysconfig/iptables

Sitten muokataan palomuurin konfiguraatio seuraavanlaiseksi:

**filter*

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

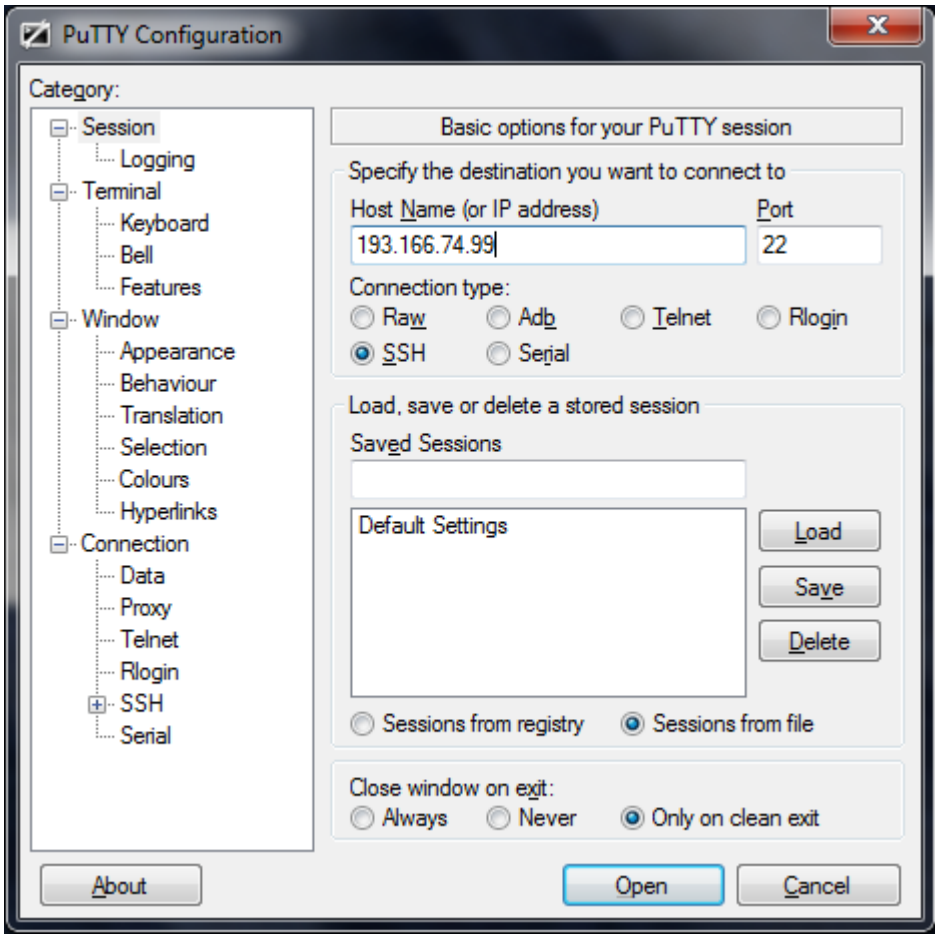
-A INPUT -j DROP

COMMIT

Jotta saadaan tehdyt muutokset voimaan, käynnistetään palomuuripalvelu uudestaan komennolla:

service iptables restart

Tämän jälkeen voidaan onnistuneesti yhdistää SSH:n kautta palvelimelle. Yhdistämiseen voidaan käyttää vaikka PuTTy-ohjelmistoa. Kuviossa 11 nähdään, kuinka PuTTy:lla avataan SSH-yhteys serveriin.



KUVIO 11. PuTTy-ohjelmalla avataan SSH-yhteys

4.3 Samba

Koska verkossa olevia käyttäjiä on vain 5, päädyttiin Sambaa toteutettaessa workgroup-palvelin ratkaisuun, jossa verkkopalvelin näkyy käyttäjille workgroupissa.

Asennetaan ensimmäisenä Samba-paketti yum:n avulla komennolla:

yum install samba

Tämän jälkeen, kun Samba on asennettu, muokataan verkkopalvelimen palomuuriasetuksia. Näin saadaan Samban tarvitsemat portit aukaistua. Avataan palomuurikonfiguraatio nano-tekstieditorilla komennolla:

nano /etc/sysconfig/iptables

Tämän jälkeen avataan palomuurista seuraavat portit: 445, 135, 137, 138, 139.

UDP-portit 137, 138 ovat NetBIOSia varten ja TCP-portit 135, 139 ja 445 ovat smbd:tä varten.

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 135 -j ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT

Tämän jälkeen tallennetaan, poistutaan ja käynnistetään iptables-palvelu uudestaan komennolla:

service iptables restart

Nyt kun portit on saatu ennakoidusti jo avattua, voidaan konfiguroida Samba. Samban konfiguraatiotiedoston avaamiseen käytetään nano-tekstieditoria ja komentoa:

nano /etc/samba/smb.conf

Seuraavaksi aloitetaan Samban konfiguroiminen. Samban konfiguraatiotiedosto on pitkä, mutta se sisältää todella paljon komentoja, joita tässä workgroup-palvelimen konfiguraatioissa ei tarvitse käyttää. Jätetään valmiskonfiguraatiot paikoilleen, mutta kommentoidaan ne pois käytöstä käyttämällä joko # tai ; -merkkiä komentorivin alussa. Ensimmäisenä muokataan [global]-osiota. Käytännössä muita osioita ei edes tarvita, sillä [global]-osion alle voidaan lisätä

kaikki komennot, joita Samban konfiguraatiossa tarvitaan. [Global]-osiossa ne vaikuttavat koko Samban konfiguraatioihin. Lisätään seuraavat komennot Samban konfiguraation [global]-osion alle

[global]

netbios name = PHKesayo

workgroup = WORKGROUP

server string = Samba Server Version %v

security = user

hosts allow = 193.166.74. 127.0.0.1

passdb backend = tdbsam

unix charset = UTF-8

local master = no

wins support = yes

ntlm auth = yes

protocol = lanman2

Avataan hieman konfiguraatiota:

- *Netbios name*: Käyttäjät näkevät workgroupissa koneen nimeltä PHKesayo.
- *Workgroup*: Määritellään työryhmän nimi. Windows-koneiden täytyy kuulua samaan työryhmään, jotta tiedostojako onnistuu.
- *Server string*: Palvelimen nimi, joka näkyy verkossa.
- *Security = user*: Asiakas ei pääse käsiksi palvelimen tietoihin, ennen kuin on syöttänyt käyttäjätunnuksen ja salasanan.
- *hosts allow*: Määritellään, mistä verkosta saa yhdistää.

- *passdb backend = tdbsam*: Määrittää salasanatietokannan, tdbsamilla voidaan hyödyntää smbpasswd:a.
- *unix charset = utf-8*: Unix-merkistö. Käytetään UTF-8-merkistöä.
- *local master = no*: Samba ei ole browsing master, eli se ei ylläpidä listaa verkkoympäristön koneiden tarjoamista palveluista ja päivitä niitä muille.
- *WINS support = yes*: Kertoo Samban NMBD-palvelulle sallia WINS server.
- *ntlm auth = yes*: Käyttää Windowsin NTLM-protokollaa tunnistautumiseen.
- *protocol = lanman2*: Käyttää lanman2-protokollaa.

Seuraavaksi käydään läpi jakokansiot. Käyttäjillä tulisi olla oma kotikansio Samballa, johon voidaan tallentaa tiedostoja ja käyttää niitä. Käyttäjille tulee luoda myös yleinen jakokansio, johon kaikilla Päijät-Hämeen kesäyliopiston työntekijöillä on oikeus kirjoittaa, ajaa ja lukea. Ensimmäisenä muokataan käyttäjien kotikansiot eli [homes]:

[homes]

comment = Kotikansiot

path = /home/%S/

browseable = yes

writable = yes

valid users = %S

guest ok = no

read only = no

Käydään kansion parametrit läpi:

path = /home/%S/ : Käyttäjän kotikansio, joka sijaitsee polussa /home/käyttäjänimi/.

browseable = yes : Kansio on selattavissa.

writable = yes : Kansioon voi kirjoittaa dataa.

valid users = %S : Sallitut käyttäjät kyseiseen kansioon eli vain kyseisellä kirjautuneella käyttäjällä on oikeus selata ja tallentaa tietoja kansioon.

guest ok = no : Vieraat eivät näe kansiota.

read only = no : Kansio ei ole vain luku -tilassa.

Koska käytetään security = user parametria, luodaan Samballe käyttäjät ja niille salasanat, jotta Windows-koneiltakin saadaan yhteys Samban kansiojakoihin. Jokaiselle käyttäjälle luodaan salasana Samban tietokantaan antamalla komento:

smbpasswd käyttäjänimi

Tämän jälkeen täytyy luoda salasana Samba-käyttäjälle. Jokaiselle käyttäjänimelle annetaan sama salasana, kuin mitä verkkopalvelimellekin on. Seuraavaksi muokataan smbusers-tiedostoa, josta löytyy kaikki Samballe luodut tunnukset. Muokataan smbusers-tiedostoa nano-editorilla:

nano /etc/samba/smbusers

 # Unix_name = SMB_name1 SMB_name2 ...

root = administrator admin

nobody = guest pcguest smbguest

tvlabra = tvlabra

admin1 = admin1

phkesayo_user1 = phkesayo_user1

phkesayo_user2 = phkesayo_user2

phkesayo_user3 = phkesayo_user3

phkesayo_user4 = phkesayo_user4

phkesayo_user5 = phkesayo_user5

Lisätään jokaisen käyttäjänimen perään = käyttäjänimi. Näin saadaan käyttäjät tunnistettua Samba-palvelimen jakoihin kirjautuessa. Jos käyttäjän tvlabra-tunnuksen perään vaihtaa esimerkiksi abralvt, täytyy tvlabra-käyttäjän kirjautua Samban verkkojakoihin Windowsista tällöin abralvt-tunnuksella. Testiympäristössä huomattiin, että kun Windowsissa ja Linuxissa on sama käyttäjätunnus ja salasana, osaa Samba yhdistää nämä toisiinsa ja jättää suorittamatta salasanakyselyn verkkojakoon siirryttäessä.

Seuraavaksi luodaan yhteiset kansiot. Nämä yhteiset kansiot täytyy kuitenkin luoda terminaalista ja antaa niille chmodilla oikeat oikeudet. Yhteisiin kansioihin halutaan antaa oikeudet niin phkesayo-ryhmälle kuin hallinta-ryhmällekin. Chmod-komennolla ei voida kuitenkaan antaa kansioon oikeuksia kahdelle eri ryhmälle, joten ensin täytyy luoda yhteinen ryhmä, jossa sijaitsevat molemmat käyttäjät. Kirjaudutaan root-tunnuksella sisään ja luodaan ryhmä. Nimetään se vaikka phkjahallinta:

groupadd phkjahallinta

Lisätään käyttäjät phkjahallinta-ryhmään seuraavalla komennolla:

usermod –aG phkjahallinta phkesayo_user1

usermod –aG phkjahallinta admin1

Näin tehdään jokaiselle käyttäjälle, jotka halutaan phkjahallinta-ryhmään, eli hallinta- ja phkesayo-ryhmän käyttäjille. Seuraavaksi luodaan yhteinen kansio, johon halutaan antaa phkjahallinta-ryhmälle oikeudet.

mkdir /usr/share/phkesayo/common

mkdir /usr/share/phkesayo/programs

Nyt luotiin kaksi kansiota, common ja programs. Seuraavaksi annetaan phkjahallinta-ryhmälle oikeudet kansioon.

chown –R root:phkjahallinta /usr/share/phkesayo/programs

chown –R root:phkjahallinta /usr/share/phkesayo/common

Seuraavaksi muutetaan chmod-komennolla kansioiden oikeuksia, jotta oikeat käyttäjät voivat muokata tiedostoja.

chmod 770 /usr/share/phkesayo/common

chmod 2770 /usr/share/phkesayo/common

Näin tehdään vielä programs-kansiollekin, jotta saadaan root-käyttäjälle ja ryhmälle täydet oikeudet kansioihin. Nyt kun oikeudet on jaettu, voidaan luoda Sambaan verkkojaot.

 # PHKesayo yhteiset

[Yhteiset tiedostot]

comment = PHKesayo yhteiset tiedostot

path = /usr/share/phkesayo/common

browseable = yes

public = yes

read only = yes

write list = @phkjahallinta

Verkossa kyseinen /usr/share/phkesayo/common -polku näkyy kansiona ’Yhteiset tiedostot’.

Pubic = yes: Tarkoittaa, että kansio on julkinen.

read only = yes: Vain luku -oikeus.

write list = @phkjahallinta: phkjahallinta-ryhmällä on oikeudet kirjoittaa kyseiseen kansioon.

Näillä annetuilla parametreillä kansio nähdään kyllä julkisena ja kansion sisällä olevia tiedostoja voidaan lukea, mutta kirjoitusoikeus kyseiseen kansioon on vain phkjahallinta-ryhmällä.

 # PHKesayo ohjelmat

[Ohjelmat]

comment = PHKK yhteiset ohjelmat

path = /usr/share/phkesayo/programs

valid users = @phkjahallinta

read only = yes

browseable = yes

public = yes

write list = @phkjahallinta

Tässä kansiossa käytetään melkein samanlaisia argumentteja, mutta hyväksytyt käyttäjät ovat phkjahallinta-ryhmän jäsenet. Kansio nähdään julkisena tiedostojaossa, mutta jos käyttäjä ei kuulu phkjahallinta-ryhmään, saa hän ilmoituksen pääsyn eväämisestä. Näin saadaan kansiot näkymään verkossa ja Samba-palvelin nähdään workgroupissa.

Windows Imaget käyttäjän tietokoneelta

Käyttäjien tietokoneista halutaan ottaa säännöllisin väliajoin image talteen mahdollisten käyttöjärjestelmien korruptioiden takia. Tällä hetkellä Windowsin imaget joudutaan ottamaan paikallisesti, mutta verkkopalvelinta voitaisiin laajentaa sovelluksella, joka osaa ottaa Windowsista varmuuskopion ja lähettää verkkokansioon.

Seuraavaksi luodaan kansio Windowsin imageille. Tähän kansioon on oikeudet vain hallinta-ryhmällä.

mkdir /usr/hallinta/winimages

chown –R root:hallinta /usr/hallinta/winimages

chmod 770 /usr/hallinta/winimages

chmod 2770 /usr/hallinta/winimages

Kun kansio on luotu ja oikeudet jaettu, luodaan kansio vielä Samban konfiguraatiotiedostoon.

 # Imageiden säilytystä varten oleva kansio

[winimages]

comment = Windows-Imageiden backupit

path = /usr/hallinta/winimages

valid users = @hallinta

browseable = no

public = no

read only = yes

write list = @hallinta

Nyt kun kansiolle on määrätty browseable = no ja public = no, kansiota ei nähdä Windows-puolella. Kun hallinta-ryhmässä tiedetään oikea polku, päästään käsiksi oikeaan kansioon. Windowsissa päästään käsiksi kansioon kirjoittamalla esimerkiksi \\PHKesayo\winimages\. Näin saadaan salattua kansio muilta kuin hallinta-ryhmän jäseniltä.

4.4 Automaattinen tiedostojen varmuuskopiointi työasemista

Palvelimella käytetään RAID-ohjainkorttia, jolla saadaan kovalevyt käyttämään RAID-tekniikkaa. Palvelimella käytetään RAID10-tekniikkaa. Kyseinen tapa yhdistää RAID1- ja RAID0-tekniikan luomalla loogiset levyt peilatuista levyistä. Tämä on erittäin suorituskykyinen ratkaisu palvelimella.

Tiedostojen varmuuskopioimiseen ei haluttu valita mitään erillistä ohjelmistoa vaan haluttiin käyttää Linuxista valmiina löytyviä toiminnallisuuksia. Linuxista löytyy helppokäyttöinen ajastuspalvelu nimeltä **cron**. Cronin ajastuksia voidaan muokata crontab-ohjelmalla.

Pelkkä cron ei kuitenkaan riitä, sillä cronia käytetään vain ajastuspalveluna. Itse varmuuskopiointi tapahtuu **tar**-sovelluksella. Tar on UNIX-järjestelmistä löytyvä pakkausohjelma, jolla voidaan pakata useampi tiedosto yhteen .tar -pakettiin. Tar-paketti pakataan pienempään kokoon käyttämällä gzip-ohjelmaa. Duplicity-sovellusta ei valittu vastaamaan varmuuskopioinnista lähinnä sen takia, että Duplicity on vielä beta-versio. Duplicityn kanssa tarvitaan myös cron-ajastus, jotta Duplicity saadaan tekemään varmuuskopiointi tiettyyn aikaan.

Palvelimelle haluttiin määritellä suhteellisen kattava varmuuskopiointi, joka ei kuitenkaan veisi liikaa tilaa kovalevyltä. Esimerkiksi, jos käyttäjiltä otettaisiin varmuuskopiot tiedostoista joka päivä, täyttyisivät palvelimen kiintolevyt todella nopeasti. Koska levytilaa on palvelimella rajoitetusti, päädyttiin seuraavanlaiseen aikajakoon:

- Neljä viikkoa kiertävä viikoittainen backup. Kun neljä viikkoa on täynnä, varmuuskopioidaan vanhimman viikkobackupin päälle ja näin saadaan jatkuva backup 4 viikon ajalta.
- Päivittäinen varmuuskopiointi viikon ajan. Kun viikko on käyty läpi, aloitetaan uusi viikko varmuuskopioimalla viime maanantaisen backupin päälle ja niin edelleen.

Tällä tavalla saadaan kaksi erillistä backupia: toinen pidemmän aikavälin backup ja toinen lyhyemmän aikavälin backup.

Kirjaudutaan sisään root-käyttäjäksi ja ajetaan seuraava komento:

crontab –e

Näin saadaan crontab auki käyttäjänä root, sillä parametri –e tarkoittaa crontab-sovelluksen suorittamista sisäänkirjautuneena käyttäjänä, eli tässä tapauksessa rootia. Kun crontabiin kirjaudutaan rootina, suoritetaan kaikki crontabissa olevat ajastuksetkin rootina. Näin saadaan varmasti oikeudet kaikkiin varmuuskopioitaviin kansioihin. Crontabiin kirjoitetaan seuraavat komennot:

@weekly /root/scripts/backup_homes_weekly /home

@weekly /root/scripts/backup_homes_weekly /usr/share/phkesayo

@daily /root/scripts/backup_homes_daily /home

@daily /root/scripts/backup_homes_daily /usr/share/phkesayo

Poistutaan tekstieditorista ja tallennetaan tiedosto. Näin ollaan saatu ajastukset kuntoon, mutta ei vielä itse varmuuskopiointia. Ajastuksissa nähdään nyt neljä komentoa, joista kaksi on viikoittain tapahtuvia ja kaksi päivittäin tapahtuvia komentoja. Viikoittain ajetaan komennot:

@weekly /root/scripts/backup_homes_weekly /home

@weekly /root/scripts/backup_homes_weekly /usr/share/phkesayo

Päivittäin ajetaan komennot:

@daily /root/scripts/backup_homes_daily /home

@daily /root/scripts/backup_homes_daily /usr/share/phkesayo

Seuraavaksi luodaan molemmille backup-metodeille oma koodi. Root-käyttäjänä luodaan kansio /root/scripts komennolla:

mkdir /root/scripts

Luodaan /root/scripts -kansioon tiedosto backup_homes_daily nano tekstieditorilla komennolla:

nano /root/scripts/backup_homes_daily

Eteen aukeaa tyhjä tekstitiedosto, jonne kirjoitetaan seuraava komentosarja:

```
#!/bin/bash

if [ "$#" -ne 1 ]; then
   echo "Not enough arguments";
   exit -1;
fi


SOURCE_DIR=$1

TARGET_DIR=/usr/backups/daily


cd $SOURCE_DIR


for D in *; do
    if [ -d "${D}" ]; then
      rm $TARGET_DIR/`date +"%w"`_${D}.tar.gz;
      tar -cvzf $TARGET_DIR/`date +"%w"`_${D}.tar.gz "${D}";
    fi
done
```

Komentosarjan alussa oleva if-lause määrittää, että komentoriviargumentteja saadaan tarpeeksi. For-loopissa olevassa komennossa käydään läpi kaikki

$SOURCE_DIR:n alla olevat kansiot. Kansiona komentosarjassa on $1, joka tässä tapauksessa tarkoittaa komentorivin ensimmäistä parametria. Tässä tapauksessa komentorivinä on crontabissa oleva:

@daily /root/scripts/backup_homes_daily /home

Ensimmäinen parametri komentorivillä on /home. $TARGET_DIR määrittää, mihin kansioon backup ajetaan. Komentosarjan for-loopissa käydään läpi kaikki /home -kansiossa olevat kansiot ja otetaan niistä backupit. Komennolla rm saadaan poistettua esim. edellisen maanantain backup ja tarilla luodaan sen hetkisen maanantain backup. Backupit tallentuvat nimellä päivämäärä+viikko_kansio.tar.gz.

Seuraavaksi luodaan /root/scripts -kansioon tiedosto backup_homes_weekly nano tekstieditorilla komennolla:

nano /root/scripts/backup_homes_weekly

Kirjoitetaan tiedostoon seuraava komentosarja:

```
#!/bin/bash


if [ "$#" -ne 1 ]; then
  echo "Not enough arguments";
  exit -1;
fi


SOURCE_DIR=$1
TARGET_DIR=/usr/backups/weekly
```

```
cd $SOURCE_DIR


for D in *; do
   if [ -d "${D}" ]; then
     WEEK=`date +"%W"`;
     rm $TARGET_DIR/$(($WEEK % 4))_${D}.tar.gz;
     tar -cvzf $TARGET_DIR/$(($WEEK % 4))_${D}.tar.gz "${D}";
   fi
done
```

Komentosarjassa käytetään samaa toimintaperiaatetta kuin backup_homes_daily-komentosarjassakin. Backupit menevät viikoittain kansioon /usr/backups/weekly. Kohdassa WEEK % 4 lasketaan viikonnumerosta jakojäännös, jolla saadaan neljän viikon sykleissä viikoittaiset backupit ajettuna koneelle. Esimerkiksi viikko 1 lasketaan 1 mod 4 = 1, 2 mod 4 = 2, 3 mod 4 = 3 ja 4 mod 4 = 0. Kun lasketaan 5 mod 1, niin saadaan taas 1, jolla ajetaan yli ensimmäisen viikon backup. Näillä kahdella komentosarjalla saadaan siis suoritettua tarvittavat backupit, niin kotikansioista kuin yhteisistä phkesayo -kansioistakin.

5 YHTEENVETO

Työn tavoitteena oli perehtyä ja suunnitella yksinkertainen verkkopalvelin pienyrityksen verkkoon. Tarkoituksena oli koota Unix-pohjainen palvelin, jossa käytettävä ohjelmisto pohjautuu avoimeen lähdekoodiin. Samalla työssä käydään läpi muutamia eri ohjelmistoja ja palveluiden tekniikoita. Työssä tavoiteltiin pienyrityksen palvelimelle sopivia palveluita ja oikeata Linux-jakelua verkkopalvelimen käyttöjärjestelmäksi.

Palvelimeen asennettiin onnistuneesti käyttöjärjestelmä sekä palvelimen palvelut. Etäyhteys saatiin toimimaan hyvin SSH:n avulla, mutta palvelinta voidaan laajentaa myöhemmin käyttämään IPSec + VPN -toteutusta, joka tarjoaa vielä turvallisemman tavan etähallita palvelinta. Palvelimeen asennetun Samban avulla saatiin onnistuneesti luotua palvelimesta workgroup-kone ja tehtyä käyttäjille verkkokansiot. Varmuuskopiointi luonnistuu crontabilla ajastetun tar-pakkausohjelman avulla.

Koottua verkkopalvelinta ei välttämättä oteta käyttöön Päijät-Hämeen kesäyliopistolla, sillä suunnitelmissa oli rakentaa uusi verkkopalvelin uusista komponenteista ja mahdollisesti kehittää siihen vielä lisäpalveluita. Opinnäytetyön konfiguraatioita voidaan hyödyntää mahdollisessa tulevassa palvelimessa.

Opinnäytetyön tarjoaman mahdollisuuden avulla päästiin tutustumaan uusin sovelluksiin sekä verkkopalvelimen ja sen eri palveluiden suunnitteluun ja toteuttamiseen. Samalla onnistuttiin myös kehittämään taitoja palvelinhallinnan ja Linux-järjestelmien kanssa, joista on varmasti hyötyä tulevaisuuden kannalta.

Linux-jakelut ovat suosituimpia käyttöjärjestelmiä palvelinkoneissa ja jopa 95 % maailman nopeimmista supertietokoneista pitää sisällään Linux-käyttöjärjestelmän. Yrityksissä käytetään Linux-palvelimia etenkin ilmaisten ohjelmistojen takia. Tällä saadaan luotua isoja säästöjä yrityksen budjetissa, kun palvelimelle tarvittavia ohjelmistoja ei tarvitse ostaa. Maksullisia Linux-jakeluita, esim. Red Hat Linuxia, käytettäessä kaikki sovellukset eivät kuitenkaan ole ilmaisia.

LÄHTEET

Barrett, D. J., Silverman, R. E. & Byrnes, R. G. 2005. SSH, The Secure Shell: The Definitive Guide, 2nd Edition. Sebastopol, CA: O'Reilly Media.

Barrett, D. J., Silverman, R. E. & Byrnes, R. G. 2013. SSH Frequently Asked Questions [viitattu 9.11.2013]. Saatavissa: http://www.snailbook.com/faq/ssh-1-vs-2.auto.html

CentOS-2. 2006. CentOS-2 Enterprise Linux 2.1AS [viitattu 11.11.2013]. Saatavissa: http://uranus.chrysocome.net/linux/centos-2/index.htm

CentOS. 2013. CentOS The Community ENTerprise Operating System [viitattu 11.11.2013]. Saatavissa: http://centos.org/

Cibernarium. 2005. Varmuuskopiointi [viitattu 12.11.2013] http://cibernarium.tamk.fi/tietoturva2/varmuuskopiointi.htm

Collier-Brown, D., Eckstein, R. & Ts, J. 2007. Using Samba, 3rd Edition. Sebastopol, CA: O'Reilly Media.

Debian Documentation Team. 2013. A Brief History of Debian [viitattu 11.11.2013]. Saatavissa: http://www.debian.org/doc/manuals/project-history/ch-intro.en.html

Debian GNU/Linux FAQ. 2013. The Debian GNU/Linux FAQ Chapter 1 - Definitions and overview [viitattu 11.11.2013]. Saatavissa: http://www.debian.org/doc/manuals/debian-faq/ch-basic_defs.en.html

Debian Wiki. 2013. Apt [viitattu 11.11.2013]. Saatavissa: https://wiki.debian.org/Apt

Duplicity. 2013. duplicity: Encrypted bandwidth-efficient backup using the rsync algorithm [viitattu 13.11.2013]. Saatavissa: http://duplicity.nongnu.org/index.html

IANA. 2013. Service Name and Transport Protocol Port Number Registry [viitattu 9.11.2013]. Saatavissa: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Linux. 2013a. CentOS [viitattu 11.11.2013]. Saatavissa: http://linux.fi/wiki/CentOS

Linux. 2013b. Dpkg [viitattu 11.11.2013]. Saatavissa: http://linux.fi/wiki/Dpkg

Linux, 2013c. Tar [viitattu 13.11.2013]. Saatavissa: http://linux.fi/wiki/Tar

Linux. 2013d. Ydin [viitattu 12.11.2013]. Saatavissa: http://linux.fi/wiki/Ydin

Microsoft Technet. 2001. Virtual Private Networking: An Overview [viitattu 9.11.2013]. Saatavissa: http://technet.microsoft.com/en-us/library/bb742566.aspx

Päijät-Hämeen kesäyliopisto. 2013. Päijät-Hämeen kesäylipisto - Sinua varten ympärivuotisesti [viitattu 10.11.2013]. Saatavissa: http://www.p-hkesayo.fi/fi/tietoa_kesayliopistosta

RFC 4250. 2006. The Secure Shell (SSH) Protocol Assigned Numbers [viitattu 9.11.2013]. Saatavissa: http://tools.ietf.org/html/rfc4250

RFC 4252. 2006. The Secure Shell (SSH) Authentication Protocol [viitattu 9.11.2013]. Saatavissa: http://tools.ietf.org/html/rfc4252

Richard Stallman. 2007. Linux and the GNU System [viitattu11.11.2013] Saatavissa: http://www.gnu.org/gnu/linux-and-gnu.html

The CentOS Project. 2013. CentOS MinimalCD 6.4 Release Notes [viitattu 11.11.2013]. Saatavissa: http://wiki.centos.org/Manuals/ReleaseNotes/CentOSMinimalCD6.4

The RAID Tutorial. 2013. Basic RAID Organizations. [viitattu 13.11.2013]. Saatavissa: http://www.ecs.umass.edu/ece/koren/architecture/Raid/basicRAID.html

VPN Consortium. 2008. VPN Technologies: Definitions and Requirements [viitattu 9.11.2013]. Saatavissa: http://www.vpnc.org/vpn-technologies.html

Wikipedia. 2013a. Comparison of Linux distributions [viitattu 11.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Comparison_of_Linux_distributions

Wikipedia. 2013b. Digital Certificates [viitattu 9.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Digital_certificates

Wikipedia. 2013c. History of Linux [viitattu 12.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/History_of_Linux

Wikipedia. 2013d. IPSec [viitattu 9.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/IPsec

Wikipedia. 2013e. Linus Torvalds [viitattu 12.11.2013]. Saatavissa: http://fi.wikipedia.org/wiki/Linus_Torvalds

Wikipedia. 2013f. Linux [viitattu 12.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Linux

Wikipedia. 2013g. Linux (ydin) [viitattu 11.11.2013]. Saatavissa: http://fi.wikipedia.org/wiki/Linux_%28ydin%29

Wikipedia. 2013h. Secure Shell [viitattu 9.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Secure_Shell

Wikipedia. 2013i. SSH [viitattu 9.11.2013]. Saatavissa: http://fi.wikipedia.org/wiki/SSH

Wikipedia. 2013j. SSH File Transfer Protocol [viitattu 9.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

Wikipedia. 2013k. Tar (computing) [viitattu 13.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Tar_%28computing%29

Wikipedia. 2013l. Ubuntu (Operating System) [viitattu 11.11.2013]. Saatavissa: http://en.wikipedia.org/wiki/Ubuntu_%28operating_system%29

Wikipedia. 2013m. Virtual Private Network [viitattu 9.11.2013] Saatavissa: http://en.wikipedia.org/wiki/Virtual_private_network

LIITTEET

LIITE 1. Samba konfigurointitiedosto smb.conf

LIITE 2. smbusers

LIITE 3. Verkkokortin asetukset

LIITE 4. Palomuuriasetukset iptables

LIITE 5. SSH Config-file sshd_config

LIITE 6. crontab + backup scripts

LIITE 7. /etc/group

LIITE 1/1. Samba konfigurointitiedosto smb.conf

```
[global]

netbios name = PHKesayo

workgroup = WORKGROUP

server string = Samba Server Version %v

security = user

hosts allow = 193.166.74. 127.0.0.1

passdb backend = tdbsam

unix charset = UTF-8

local master = no

wins support = yes

ntlm auth = yes

protocol = lanman2

[homes]

        comment = Kotikansiot

        path = /home/%S/

        browseable = yes

        writable = yes

        valid users = %S

        guest ok = no

        read only = no
```

LIITE 1/2.

```
# PHKesayo yhteiset

        [Yhteiset tiedostot]

        comment = PHKesayo yhteiset tiedostot

        path = /usr/share/phkesayo/common

        browseable = yes

        public = yes

        read only = yes

        write list = @phkjahallinta


# PHKesayo ohjelmat

        [Ohjelmat]

        comment = PHKK yhteiset ohjelmat

        path = /usr/share/phkesayo/programs

        valid users = @phkjahallinta

        read only = yes

        browseable = yes

        public = yes

        write list = @phkjahallinta
```

```
# Imageiden säilytystä varten oleva kansio

    [winimages]

    comment = Windows-Imageiden backupit

    path = /usr/hallinta/winimages

    valid users = @hallinta

    browseable = no

    public = no

    read only = yes

    write list = @hallinta
```

LIITE 2. smbusers

```
# Unix_name = SMB_name1 SMB_name2 ...

root = administrator admin

nobody = guest pcguest smbguest

tvlabra = tvlabra

admin1 = admin1

phkesayo_user1 = phkesayo_user1

phkesayo_user2 = phkesayo_user2

phkesayo_user3 = phkesayo_user3

phkesayo_user4 = phkesayo_user4

phkesayo_user5 = phkesayo_user5

phkesayo_user6 = phkesayo_user6
```

LIITE 3. Verkkokortin asetukset

/etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

IPADDR=193.166.74.99

NETMASK=255.255.255.128

NETWORK=193.166.74.0

BROADCAST=193.166.74.127

HWADDR=00:0C:76:AD:83:43

TYPE=Ethernet

UUID=0e366376-d237-4c5e-bda6-f09590f00b71

ONBOOT=yes

NM_CONTROLLED=no

BOOTPROTO=none

USERCTL=no

LIITE 4/1. Palomuuriasetukset iptables

```
# Firewall configuration written by system-config-firewall

# Manual customization of this file is not recommended.

*filter

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

# Samban portin aukaisua.

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 445 -j
ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m udp -p udp --dport 445 -j
ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 135 -j
ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m udp -p udp --dport 137 -j
ACCEPT

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m udp -p udp --dport 138 -j
ACCEPT
```

LIITE 4/2.

-A INPUT -s 193.166.74.0/25 -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT

-A INPUT -j DROP

COMMIT

LIITE 5/1. SSH Config-file sshd_config

```
#	$OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
```

LIITE 5/2.

activation of protocol 1

Protocol 2

HostKey for protocol version 1

#HostKey /etc/ssh/ssh_host_key

HostKeys for protocol version 2

#HostKey /etc/ssh/ssh_host_rsa_key

#HostKey /etc/ssh/ssh_host_dsa_key

Lifetime and size of ephemeral version 1 server key

#KeyRegenerationInterval 1h

#ServerKeyBits 1024

Logging

obsoletes QuietMode and FascistLogging

#SyslogFacility AUTH

SyslogFacility AUTHPRIV

#LogLevel INFO

LIITE 5/3.

```
# Authentication:


#LoginGraceTime 2m
PermitRootLogin no
StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
```

LIITE 5/4.

#IgnoreUserKnownHosts no

Don't read the user's ~/.rhosts and ~/.shosts files

IgnoreRhosts yes

To disable tunneled clear text passwords, change to no here!

#PasswordAuthentication yes

PermitEmptyPasswords no

PasswordAuthentication yes

Change to no to disable s/key passwords

#ChallengeResponseAuthentication yes

ChallengeResponseAuthentication no

Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

#KerberosUseKuserok yes

LIITE 5/5.

```
# GSSAPI options

#GSSAPIAuthentication no

GSSAPIAuthentication yes

#GSSAPICleanupCredentials yes

GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no


# Set this to 'yes' to enable PAM authentication, account processing,

# and session processing. If this is enabled, PAM authentication will

# be allowed through the ChallengeResponseAuthentication and

# PasswordAuthentication.  Depending on your PAM configuration,

# PAM authentication via ChallengeResponseAuthentication may bypass

# the setting of "PermitRootLogin without-password".

# If you just want the PAM account and session checks to run without

# PAM authentication, then enable this but set PasswordAuthentication

# and ChallengeResponseAuthentication to 'no'.

#UsePAM no

UsePAM yes
```

LIITE 5/6.

```
# Accept locale-related environment variables

AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE
LC_MONETARY LC_MESSAGES

AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE
LC_MEASUREMENT

AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE

AcceptEnv XMODIFIERS


#AllowAgentForwarding yes

#AllowTcpForwarding yes

#GatewayPorts no

X11Forwarding no

#X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

#PrintMotd yes

#PrintLastLog yes

#TCPKeepAlive yes

#UseLogin no

#UsePrivilegeSeparation yes

#PermitUserEnvironment no
```

LIITE 5/7.

```
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10
#PermitTunnel no
#ChrootDirectory none

# no default banner path
#Banner none
# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       ForceCommand cvs server
```

LIITE 6/1. crontab + backup scripts

crontab

```
@weekly /root/scripts/backup_homes_weekly /home

@weekly /root/scripts/backup_homes_weekly /usr/share/phkesayo

@daily /root/scripts/backup_homes_daily /home

@daily /root/scripts/backup_homes_daily /usr/share/phkesayo
```

root/scripts/backup_homes_daily

```
#!/bin/bash

if [ "$#" -ne 1 ]; then

  echo "Not enough arguments";

  exit -1;

fi

SOURCE_DIR=$1

TARGET_DIR=/usr/backups/daily

cd $SOURCE_DIR

for D in *; do

   if [ -d "${D}" ]; then

     rm $TARGET_DIR/`date +"%w"`_${D}.tar.gz;

     tar -cvzf $TARGET_DIR/`date +"%w"`_${D}.tar.gz "${D}";

   fi
```

LIITE 6/2.

```
done
```

/root/scripts/backup_homes_weekly

```
#!/bin/bash

if [ "$#" -ne 1 ]; then
   echo "Not enough arguments";
   exit -1;
fi
SOURCE_DIR=$1
TARGET_DIR=/usr/backups/weekly
cd $SOURCE_DIR
for D in *; do
    if [ -d "${D}" ]; then
      WEEK=`date +"%W"`;
      rm $TARGET_DIR/$(($WEEK % 4))_${D}.tar.gz;
      tar -cvzf $TARGET_DIR/$(($WEEK % 4))_${D}.tar.gz "${D}";
    fi
done
```

LIITE 7/1. /etc/group

root:x:0:

bin:x:1:bin,daemon

daemon:x:2:bin,daemon

sys:x:3:bin,adm

adm:x:4:adm,daemon

tty:x:5:

disk:x:6:

lp:x:7:daemon

mem:x:8:

kmem:x:9:

wheel:x:10:

mail:x:12:mail,postfix

uucp:x:14:

man:x:15:

games:x:20:

gopher:x:30:

video:x:39:

dip:x:40:

ftp:x:50:

lock:x:54:

LIITE 7/2.

audio:x:63:

nobody:x:99:

users:x:100:

floppy:x:19:

vcsa:x:69:

utmp:x:22:

utempter:x:35:

cdrom:x:11:

tape:x:33:

dialout:x:18:

saslauth:x:76:

postdrop:x:90:

postfix:x:89:

fuse:x:499:

sshd:x:74:

wbpriv:x:88:

testi:x:500:

hallinta:x:501:

phkesayo:x:502:

phkjahallinta:x:503:phkesayo_user1,phkesayo_user2,phkesayo_user3,phkesayo_user4,phkesayo_user5,admin1,tvlabra

LIITE 7/3.

tcpdump:x:72: